REMARKS

Claims 1-65 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 103(a) Rejection:

The Examiner rejected claims 1-65 under 35 U.S.C. § 103(a) as being unpatentable over Huitema et al. (U.S. Publication 2003/0056093) (hereinafter "Huitema") in view of Klonowski (U.S. Patent 5,479,514). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 1, contrary to the Examiner's assertion, Huitema in view of Klonowski fails to teach or suggest *the second peer generating a first session key from the first public key.* The Examiner cites FIG. 3 and paragraph [0054] of Huitema as teaching *a first peer sending a message to a second peer on a peer-to-peer network, wherein the message indicates that the first peer is requesting a session with the second peer;* and FIGs. 3-5 and paragraphs [0055-56] of Huitema as teaching *the first peer sending a first public key to the second peer; the second peer receiving the first message; the second peer receiving the first public key;* and *the second peer determining if a session with the first peer is to be established in response to the message indicating the first peer is requesting a session with the second peer.* These figures and passages describe a method for forming a peer-to-peer group in which a peer group Owner invites a member U1 to join the group. The Owner sends an invitation to U1 that contains the Group PNRP ID and Group certificate 212, which the Owner created (see paragraph [0052]), containing U1's public key signed with the Group Private Key. Once U1 receives the invitation, the Examiner's citations describe the steps taken to complete the process of joining the group. In other words, the Group Owner (which, in citing paragraph [0054], the Examiner appears to equate with the first peer of Applicants' claim 1) sends an invitation to U1 (the second peer according to the Examiner) to join a peer group via email. The process of joining the group then involves exchanging a Group

certificate, created by the Owner (the first peer per the Examiner, see paragraph [0052]). This citation teaches away from Applicants' invention, in that the group Owner (the first peer), and not an individual peer invited to join a group (the second peer), generates a key to be used when communicating between group members.

The Examiner first appears to equate Applicants first peer to the Owner and Applicants second peer to node U1 when the Examiner refers to paragraph [0054]. But when citing paragraphs [0055-0056], the Examiner appears to re-assign the roles of the first and second peers. The Examiner changes to equating node U1 with the first peer of claim 1 and node U2 with the second peer of claim 1. This is inconsistent with the Examiner's reliance in citing paragraph [0054] that the Owner is analogous to Applicants' first peer and node U1 is analogous to Applicants' second peer. Clearly, these two interpretations cannot be applied simultaneously. Furthermore, using the second interpretation, Huitema still does not teach or suggest the second peer (U2) generating any type of key to be used in communications between the two peer nodes, U1 and U2. Instead, Huitema teaches that U2 may send its Group Certificate (generated by the Owner) to U1 to prove its group membership, and then may send the group's current shared key (also generated by the Owner, as described in [0052]) to U1.

The Examiner admits that Huitema fails to explicitly disclose *a session key* and relies on Klonowski to teach this limitation. Specifically, the Examiner cites Klonowski (column 6, lines 13-16). This citation in Klonowski describes a secure network in which a secondary logical unit (SLU) replies to a LOCATE request from a primary logical unit (PLU) seeking to establish a session with the SLU. The SLU may generate a session key and include this in its reply. However, this passage does not describe that the session key is generated from the first public key, i.e., one that was sent to the second peer (SLU) by the first peer (PLU), as in claim 1, "*the first peer sending a first public key to the second peer*". **Nothing in the Examiner's citations, or elsewhere in Huitema or Klonowski, alone or combined, teaches or suggests *the second peer generating a first session key from the first public key*, as recited in claim 1.** In Huitema, the key is generated by the Owner, not the second peer. Furthermore, neither the Owner nor the second peer in

Huitema generate the key from the public key received from the first peer. In Klonowski, although the SLU does generate a key, it does not generate a key from a public key received from the PLU or any other node. **Therefore, no combination of Huitema and Klonowski could possibly be considered to teach or suggest the second peer generating a first session key from the first public key received from the first peer node, as recited in claim 1.**

> In the Response to Arguments section of the Final Action, the Examiner asserts:
>
> Klonowski discloses a secure network data communication technique by using an advanced peer-to-peer networking (APPN) system. The advanced peer-to-peer networking system provides communication such as message routing, which allows session establishment and routing services between the first peer and the second peer. When an APPN node (first peer) wishes to establish a session with another node (second peer), the first peer initiates a request. (See Figure 6 and Column 5, lines 56-65). This determination is made through the use of sharing keys between the two peers to the network node hosting the second peer. The network node initiates a request communication by transmitting it into the network. In response, the second peer receives a message indicating that the first peer is requesting a session with the second peer. (See Column 6, lines 6-12). Therefore, if it is determined that a secured session is to be established, then a session key may be generated and sent to the first peer in a message (See Column 6, lines 13-28).

Again, these citations do not teach or suggest *the second peer generating a first session key from the first public key*, as recited in claim 1. There is nothing in this passage, or elsewhere in Huitema or Klonowski or in the combination thereof, that teaches or suggests the second peer generating a first session key from the first public key received from the first peer node. Similar remarks apply also to independent claims 15, 33, 45 and 56, each of which recites limitations involving a second peer generating a first session key from a first public key, wherein the first public key was sent to the second peer by a first peer.

Moreover, Applicants' claim 1 recites that generation of a session key by the second peer is conditioned on determination by the second peer that a session is to be established. The REPLY in Klonowski is explicitly **not** conditioned on the second

peer determining if a session is to be established. Klonowski specifically requires that the second peer sends a REPLY, including an encrypted session key, to the PLU (first node) as soon as it is located. **Thus, the cited art actually teaches away from Applicants' claimed invention.**

The Examiner's remarks in the Response to Arguments indicate that "This determination is made through the use of sharing keys between the two peers to the network node hosting the second peer..." However, this "determination" in Klonowski is by the first peer that it would like to contact the second peer to request a session. The cited art does not describe such a determination by the second peer. The Examiner's remarks also include "if it is determined that a secured session is to be established, then a session key may be generated and sent to the first peer in a message" (emphasis added). This statement by the Examiner is entirely unsupported by the actual teachings of the cited art. **Nowhere does Klonowski teach that the generation and sending of a first session key by the second peer is conditioned on the second peer determining if a secured session is to be established. To the contrary, the cited art specifically teaches that the second peer always sends a REPLY to the LOCATE.**

Furthermore, there is no motivation found in the prior art to modify the teachings of Huitema according to Klonowski as proposed by the Examiner. The Examiner contends that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Huitema's peer-to-peer group method by using Klonowski's encrypted communication because Klonowski provides a secure method for data to be exchanged within a peer-to-peer communication by incorporating a session key. The Examiner cites Klonowski, column 2, lines 23-35 as providing this motivation. This citation describes that the invention of Klonowski "solves the security problem with vendor independent nodes and simultaneously mitigates the problem of key proliferation in APPN networks." However, neither of these problems is described as being present in the system of Huitema. Applicants remind the Examiner that, "It is well-established that before a conclusion of obviousness may be made based on a combination of references, there must have been a reason, suggestion, or motivation to lead an

inventor to combine those references." *Pro-Mold and Tool Co. v. Great Lakes Plastics Inc.*, 75 F.3d 1568, 1573, 37 USPQ2d 1626, 1629 (Fed. Cir. Feb. 1996). Furthermore, the infrastructure and method of Huitema already provide a secure method for data to be exchanged through various disclosed methods involving peer-to-peer groups and security credentials and protocols thereof (see Huitema, abstract). Therefore, there would be no motivation to provide a different way to provide secure data exchange in Huitema.

Moreover, modifying the peer-to-peer group methods of Huitema so that a second peer generates a session key as in Klonowski would change the principal of operation in the system of Huitema, in which secure communications are managed through peer group membership and peer group protocols with keys supplied only by a group Owner. For example, the peer group methods of Huitema specifically depend on a group Owner to create a Group Certificate and group shared keys, and to decide who may join the peer group. In Huitema's system, secure peer-to-peer communications are ensured because individual peers cannot establish communication with each other outside of this Owner-managed peer group methodology. Klonowski, on the other hand, teaches a system in which two nodes independently establish a communication session with each other, without any such peer group ownership or management. Moreover, the method of Huitema is specifically directed to group communications. In contrast, the secure technique of Klonowski applies only to communications between the PLU node and SLO node, not a group. Therefore, Klonowski's methods are not combinable with Huitema's system, as they are completely incompatible with the basic operating principles of Huitema. As stated in the MPEP §2143.01 "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti* , 270 F.2d 810, 123 USPQ 349 (CCPA 1959). . ." (*emphasis added*). As shown above, the references actually teach away from their combination.

The Examiner rejected claims 25 and 29 along with claim 1. **However, these claims recite different limitations than claim 1, which are not addressed by the Examiner in his remarks. Therefore, the rejection of these claims is improper.**

Regarding claim 25, Huitema in view of Klonowski fails to teach or suggest *generating one or more session keys from one or more public keys of the plurality of peers... wherein there are one or more unique pairs of the plurality of peers, wherein each unique pair of the plurality of peers shares a particular one of the one or more session keys, wherein the particular session key is generated from a public key of one of the particular pair of peers, and wherein only the particular pair of peers possesses the particular session key.* As discussed above regarding claim 1, Huitema depends on a peer group methodology to provide secure communication through a Group Certificate and group shared keys. Huitema does not accommodate an individual pair of peers participating in a communication session having its own key, i.e., one that is possessed only by the particular pair of peers in the session, rather than by an entire peer group. In addition, the Examiner admits that Huitema does not teach the *session key* feature of Applicants' invention and relies on Klonowski to teach this limitation. As discussed above, Klonowski's session keys are not generated from a public key of one of the two participants in a session. Therefore, Huitema in view of Klonowski fails to teach or suggest all of the limitations of Applicants' claim 25. Furthermore, the session key feature of Klonowski has been shown to be incompatible, and therefore not combinable, with the peer group methodology of Huitema, as it **teaches away from** the principles of operation of Huitema.

For at least the reasons above, the rejection of claim 25 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 29, Huitema in view of Klonowski fails to teach or suggest *a plurality of peers in a peer-to-peer network joining in a session* and *generating a session key from a public key of a first of the plurality of peers.* As discussed above regarding claims 1 and 25, there is nothing in Huitema or Klonowski, taken alone or in

combination, that teaches or suggests generating a session key from a public key of one the peers joining in a session. As discussed above regarding claim 1, Huitema depends on a group Owner generating shared keys and Group Certificates for security. Also as discussed above, Klonowski's session keys are not generated from a public key of a session participant. Therefore, Huitema in view of Klonowski fails to teach or suggest all of the limitations of Applicants' claim 29. Furthermore, as discussed above regarding claims 1 and 25, the session key feature of Klonowski is not combinable with the peer group methodology of Huitema, as it **teaches away from** the principles of operation of Huitema.

For at least the reasons above, the rejection of claim 29 is not supported by the cited art and removal thereof is respectfully requested.

Applicants also assert that numerous ones of the dependent claims recite further distinctions over the cited art. However, since the rejection has been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

CONCLUSION

Applicants submit the application is in condition for allowance, and prompt notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-94200/RCK.

Also enclosed herewith are the following items:

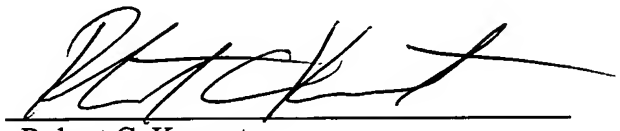
☒ Return Receipt Postcard

☐ Petition for Extension of Time

☐ Notice of Change of Address

☐ Other:

Respectfully submitted,



Robert C. Kowert
Reg. No. 39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: June 7, 2006